

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Ito et al.

Express Mail: EF297166669US

Filed: January 3, 2001

Group No.:

Examiner:



For: CONTROL PROGRAM, DEVICE INCLUDING THE CONTROL PROGRAM,
METHOD FOR CREATING THE CONTROL PROGRAM, AND METHOD FOR
OPERATING THE CONTROL PROGRAM

Assistant Commissioner for Patents
Washington, D.C. 20231

TRANSMITTAL OF CERTIFIED COPY

Attached please find the certified copy of the foreign application from which
priority is claimed for this case:

Country: Japan
Application Number: 2000-005501
Filing Date: January 14, 2000


SIGNATURE OF ATTORNEY

Reg. No. 26,725

Neil A. DuChez

Tel. No. (216) 621-1113

RENNER, OTTO, BOISSELLE & SKLAR, P.L.L.
1621 Euclid Avenue
Nineteenth Floor
Cleveland, Ohio 44115

(Translation)
PATENT OFFICE
JAPANESE GOVERNMENT

1c918 U.S. PRO
09/754018
01/03/01

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application : January 14, 2000

Application Number : Patent Appln. No. 2000-005501

Applicant(s) : MATSUSHITA ELECTRIC INDUSTRIAL CO.,
LTD.

Wafer
of the
Patent
Office

December 8, 2000

Kozo OIKAWA

Commissioner,
Patent Office

Seal of
Commissioner
of
the Patent
Office

Appln. Cert. No.

Appln. Cert. Pat. 2000-3103202

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

1c918 U.S. PTO
09/754018
01/03/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出 願 年 月 日
Date of Application:

2000年 1月14日

出 願 番 号
Application Number:

特願2000-005501

出 願 人
Applicant (s):

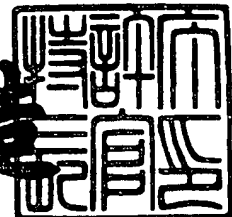
松下電器産業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年12月 8日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2000-3103202

【書類名】 特許願

【整理番号】 2032410442

【提出日】 平成12年 1月14日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00
G11B 20/00

【発明者】

 【住所又は居所】 大阪府門真市大字門真1 0 0 6 番地 松下電器産業株式
 会社内

 【氏名】 伊藤 基志

【発明者】

 【住所又は居所】 大阪府門真市大字門真1 0 0 6 番地 松下電器産業株式
 会社内

 【氏名】 植田 宏

【発明者】

 【住所又は居所】 大阪府門真市大字門真1 0 0 6 番地 松下電器産業株式
 会社内

 【氏名】 佐々木 真司

【特許出願人】

 【識別番号】 000005821

 【氏名又は名称】 松下電器産業株式会社

【代理人】

 【識別番号】 100097445

 【弁理士】

 【氏名又は名称】 岩橋 文雄

【選任した代理人】

 【識別番号】 100103355

 【弁理士】

 【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【書類名】 明細書

【発明の名称】 制御プログラム隠蔽方法および制御プログラムが隠蔽された装置

【特許請求の範囲】

【請求項 1】 データを変換するデータ変換回路を備えた装置の制御プログラム隠蔽方法であって、

制御プログラムの一部に前記データ変換回路の逆変換を施すプログラム逆変換ステップと、

前記プログラム逆変換ステップにより一部が逆変換された制御プログラムをプログラムメモリに格納するプログラム格納ステップと、
を包含することを特徴とする制御プログラム隠蔽方法。

【請求項 2】 データを変換するデータ変換回路を備えた装置の制御プログラム隠蔽方法であって、

制御プログラムの一部である対象プログラムをプログラムメモリから書換可能メモリにコピーするプログラム複製ステップと、

前記プログラム複製ステップによりコピーされた対象プログラムを前記データ変換回路によって変換するプログラム変換ステップと、

前記プログラム変換ステップにより変換された対象プログラムを実行するプログラム実行ステップと

を包含することを特徴とする制御プログラム隠蔽方法。

【請求項 3】 前記制御プログラム隠蔽方法は、前記プログラム変換ステップにより変換された対象プログラムの実行が終了した後に、前記対象プログラムを書換可能メモリから消去するプログラム消去ステップをさらに包含する、請求項 2 に記載の制御プログラム隠蔽方法。

【請求項 4】 請求項 2 または請求項 3 に記載の制御プログラムを備えた装置

。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、装置組込み型の制御プログラムを隠蔽する方法および制御プログラムが隠蔽された装置に関するものである。

【 0 0 0 2 】

【従来の技術】

近年、音楽や映像といったコンテンツがデジタル化される中で、著作権を保護する重要度が増している。そこで、コンテンツを暗号化する手法が用いられている。この暗号化されたコンテンツを再生するには、暗号を解読する必要がある。そこで、再生装置を開発するために、ライセンスを結んで、暗号の解読方法入手するのであるが、同時に解読方法が外に漏れないように、何らかの保護手段を講じて装置に組み入れることが求められる。

【 0 0 0 3 】

解読方法が L S I などのハードウェアに組み込まれている場合、L S I の製造技術をもつ専門の人でないかぎり、L S I 中のアルゴリズムを解析することは不可能である。しかしながら、暗号方式がソフトウェアによって組み込まれている場合、そのソフトウェアの実行ファイルから逆アセンブルなどで解析できる人、いわゆるハッカーと呼ばれる人達がいる。そうしたハッカーに対抗すべく、解析され難いソフトウェア (T a m p e r R e s i s t a n t P r o g r a m) の技術がある。

【 0 0 0 4 】

【発明が解決しようとする課題】

しかしながら、L S I などのハードウェアによる解読方法の組込みは、近年の開発競争においては、開発速度面とコスト面で不利に働く傾向がある。また、ソフトウェア技術だけによる保護は、ソフトウェア技術で解析が不可能とは言えない。

【 0 0 0 5 】

本発明は上記問題点に鑑み、装置組込み型の制御プログラムの特徴を生かした、ハードウェアとソフトウェアを組み合わせたプログラムの隠蔽方法を提供する。

【 0 0 0 6 】

【課題を解決するための手段】

本発明の制御プログラム隠蔽方法は、データを変換するデータ変換回路を備えた装置の制御プログラム隠蔽方法であって、制御プログラムの一部に前記データ変換回路の逆変換を施すプログラム逆変換ステップと、前記プログラム逆変換ステップにより一部が逆変換された制御プログラムをプログラムメモリに格納するプログラム格納ステップとを包んでおり、これにより上記目的が達成される。

【0007】

本発明の制御プログラム隠蔽方法は、データを変換するデータ変換回路を備えた装置の制御プログラム隠蔽方法であって、制御プログラムの一部である対象プログラムをプログラムメモリから書換可能メモリにコピーするプログラム複製ステップと、前記プログラム複製ステップによりコピーされた対象プログラムを前記データ変換回路によって変換するプログラム変換ステップと、前記プログラム変換ステップにより変換された対象プログラムを実行するプログラム実行ステップとを包んでおり、これにより上記目的が達成される。

【0008】

前記制御プログラム隠蔽方法は、さらに、前記プログラム変換ステップにより変換された対象プログラムの実行が終了した後に、前記対象プログラムを書換可能メモリから消去するプログラム消去ステップを包んでおり、これにより上記目的が達成される。

【0009】

【発明の実施の形態】

以下、図面を参照しながら本発明の実施の形態を説明する。

【0010】

図1は、本発明の実施の形態における装置の構成の一例を示すブロック図である。図1で示される装置1は、不揮発性メモリであるプログラムメモリ4と、プログラムメモリ4に格納された制御プログラムに従って装置1を制御する小型演算素子(MPU: Micro Processor Unit)であるマイコン2と、マイコン2の作業データ等を一時的に格納する書換可能メモリであるDRAM5と、データを可逆的に変換するデータ変換回路3と、その他の回路6と、

それらを接続する内部バス 7 から構成される。ここで、不揮発性メモリとしては、再生専用メモリや 1 回書込可能メモリ (One Time ROM) やフラッシュメモリなどがある。書換可能メモリとしては、データの保持動作が不要なスタティックメモリ (Static Memory) やデータの保持動作が必要なダイナミックメモリ (Dynamic Memory) などがある。その他の回路としては、例えば情報記憶装置の場合は、データ誤り訂正回路などがある。

【0011】

図 2 は、データ変換回路 3 の一例を示す回路図である。図 2 において、四角が 1 ビットのフリップフロップで、丸が 1 ビットの排他的論理和であり、基本的にクロック 1 周期で左側に 1 ビットずつデータを移動するシフトレジスタのようなものである。これは、エラー訂正理論で用いられる 8 次の原始多項式 (Primitive polynomial) である $P(x) = x^8 + x^4 + x^3 + x^2 + 1$ を表している。図 2 の左端のフリップフロップ (x^0 で示される) に 1、その他のフリップフロップに 0 を初期設定し、1 クロック毎に出力されるデータ列を 16 進数で表記すると、01, 02, 04, 08, 10, 20, 40, 80, 1D, 3A, . . . , 8E, 01, . . . の 255 回 ($= 2^8 - 1$ 回) で周期的なデータ列となる。この出力データ列に 256 回目を 00 として加えれば、可逆的な 8 ビットのデータ変換ができる。そのデータ変換を 16 進数であらわすと、00 は 01、01 は 02、02 は 04、03 は 08, . . . , FE は 8E、FF は 00 となる。またデータ逆変換は、00 は FF、01 は 00、02 は 01、03 は 19, . . . , FE は 58、FF は AF となる。但し、これはデータ変換の一例にすぎず、可逆的なデータ変換ができれば、どのような回路であってもよい。エラー訂正回路を備えた装置であれば、このような可逆データ変換が誤り訂正回路に予め存在するので、誤り訂正回路をデータ変換回路として流用することも可能である。

【0012】

図 3 は、部分的に隠蔽されたプログラムの実行形式の作成フローチャートである。

【0013】

(301) 隠蔽すべき制御手順をプログラミングし、隠蔽の対象となるプログラムソース311を作成する。

【0014】

(302) 作成されたプログラムソース311をコンパイルおよびリンクして、実行形式のバイナリデータ312を生成する。

【0015】

(303) 実行形式のバイナリデータ312に、上述したデータ逆変換を施して、逆変換済みのバイナリデータ313を生成する。

【0016】

(304) 逆変換済みのバイナリデータ313を、他のプログラムソースに組み入れやすいように、プログラムソース形式（例えばC言語のchar型の配列表記を内容として持つインクルードファイル形式）である、逆変換済みのバイナリデータを表現するデータ配列314に変換する。

【0017】

(305) 逆変換済みのバイナリデータを表現するデータ配列314と隠蔽対象でない他の制御手順とを結合し、全プログラムソース315を作成する。

【0018】

(306) 全プログラムソース315をコンパイルおよびリンクして、装置のプログラムメモリ4に格納される実行形式のバイナリデータ316を生成する。

【0019】

上述したバイナリデータ316は、予めプログラムメモリ4に書込まれて出荷されることもあるし、最近のパーソナルコンピュータのマザーボードで見かけられるように、フラッシュメモリを用いたプログラムメモリを更新するために、インターネット経由でバイナリデータ316の最新バージョンが配布されることもある。バイナリデータ316は、例え逆アセンブルといった手法を用いても、隠蔽された制御手順を解析することはできない。

【0020】

図4は、隠蔽されたプログラムの実行フローチャートである。図5で示した隠蔽されたプログラムの領域を示した図と合わせて説明する。

【 0 0 2 1 】

(4 0 1) 図 5 A で示されるように、プログラムメモリ 4 に格納された隠蔽されたプログラム 5 0 1 を、D R A M 5 に複製し、複製プログラム 5 0 2 を作る。

【 0 0 2 2 】

(4 0 2) 図 5 B で示されるように、D R A M 5 上の複製プログラム 5 0 2 を、データ変換回路 3 を用いて、復元プログラム 5 0 3 に復元する。

【 0 0 2 3 】

(4 0 3) 図 5 B で示される復元プログラム 5 0 3 の中の関数（モジュールとも呼ぶ）を呼び出す。関数の呼び出しに関する詳細は後述する。

【 0 0 2 4 】

(4 0 4) 呼び出した関数から戻ってきた後に、図 5 C で示されるように、復元プログラム 5 0 3 が存在した領域 5 0 4 を、値 0 で埋めるなどして消去する。

【 0 0 2 5 】

ステップ (4 0 2) の復元処理を、全てソフトウェアで実行する場合、この箇所を解析されれば、隠蔽されたプログラムが解読される危険性がある。本発明の実施の形態では、装置 1 に固有のハードウェアであるデータ変換回路 3 を用いることで、隠蔽されたプログラムを解読から守ることができる。

【 0 0 2 6 】

次に、関数の呼び出し方法について説明する。図 6 は、隠蔽対象のプログラムの構造を示す図である。隠蔽対象のプログラムは、外部から呼び出される公開関数 6 1 と 6 2 と、内部から相対番地で呼び出される内部関数 6 3 と 6 4 と 6 5 と、隠蔽対象のプログラムの先頭からみた公開関数 6 1 と 6 2 の相対番地を列挙した相対番地リスト 6 0 から構成される。これらの番地の情報は、図 5 A の複製プログラム 5 0 2 の位置に依存しない情報であり、図 3 の対象プログラムソース 3 1 1 から得ることができる。

【 0 0 2 7 】

図 7 は、マイコン 2 から見たアドレス空間を示す図である。プログラムメモリ 4 と D R A M 5 は、マイコン 2 から見ると、それぞれ独自の番地が割付けられた領域に配置される。逆変換されたプログラム（図 7 中のプログラムメモリのハン

チングされた領域）から複製され復元された復元プログラム（図 7 中の D R A M のハンチングされた領域）は、マイコン 2 が指定した所定の番地（図 7 中の複製した先頭番地）から配置される。従って、公開関数 1 のマイコンから見た絶対番地は、複製した先頭番地に公開関数 1 の相対番地を加算することによって求められる。この絶対番地を指定することで、公開関数 1 を呼び出すことができる。公開関数 2 についても同様である。

【 0 0 2 8 】

【発明の効果】

以上説明したように、本発明の実施の形態によれば、部分的に隠蔽された制御プログラムを作成でき、この隠蔽された制御プログラムを安全に復元して実行することができる。プログラムの復元アルゴリズムは、装置に組み込まれたハードウェアとで分担しているので、非常に高度なソフトウェア技術を有した人物であっても、制御プログラムだけを解析しても分からない。用いるハードウェアは簡単な回路でも、十分な解読に対する抵抗力を持つことができるので、隠蔽すべき処理を全てのハードウェアで実現したり、もしくは全てソフトウェアで実現するのに比較して、開発期間とコストと安全性の面で優れている。

【図面の簡単な説明】

【図 1】

本発明の実施の形態における装置の構成の一例を示すブロック図

【図 2】

データ変換回路の一例を示す回路図

【図 3】

部分的に隠蔽されたプログラムの実行形式の作成フローチャート

【図 4】

隠蔽されたプログラムの実行フローチャート

【図 5 A】

プログラム複製処理におけるプログラム領域の配置図

【図 5 B】

プログラム変換処理におけるプログラム領域の配置図

【図 5 C】

プログラム消去処理におけるプログラム領域の配置図

【図 6】

隠蔽対象のプログラムの構造図

【図 7】

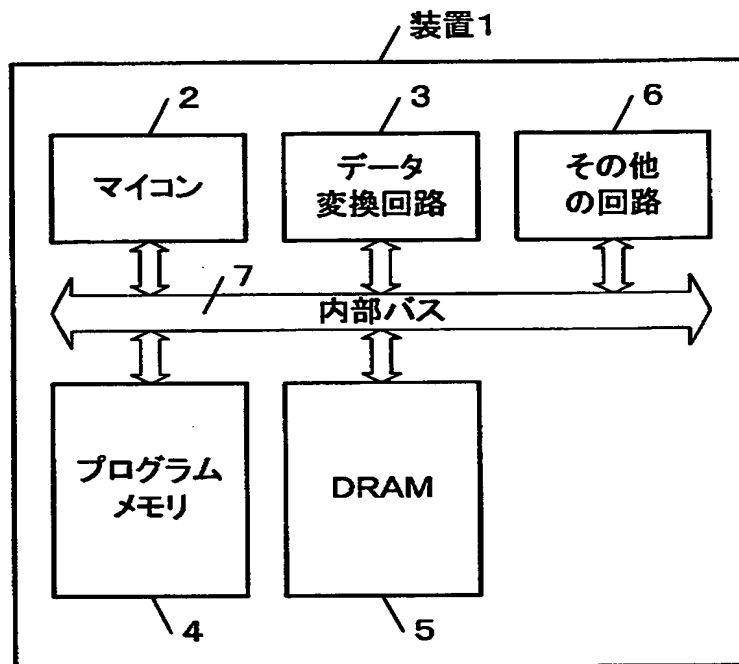
マイコンから見たアドレス空間図

【符号の説明】

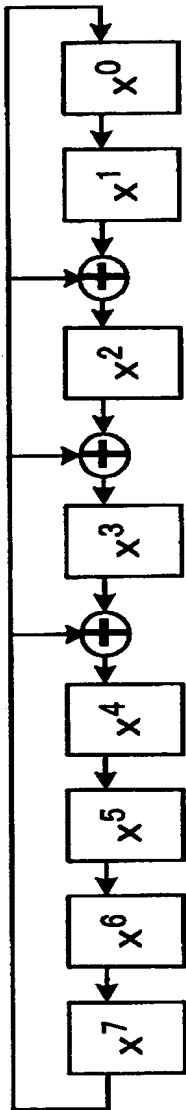
- 1 装置
- 2 マイコン
- 3 データ変換回路
- 4 プログラムメモリ
- 5 DRAM
- 6 その他の回路
- 7 内部バス
- 60 相対番地リスト
- 61, 62 公開関数
- 63, 64, 65 内部関数
- 311 対象プログラムソース
- 312 実行形式のバイナリデータ
- 313 逆変換済みのバイナリデータ
- 314 逆変換済みのバイナリデータを表現するデータ配列
- 315 全プログラムソース
- 316 プログラムメモリに格納される実行形式のバイナリデータ
- 501 隠蔽されたプログラム
- 502 複製プログラム
- 503 復元プログラム
- 504 消去されたプログラム領域

【書類名】 図面

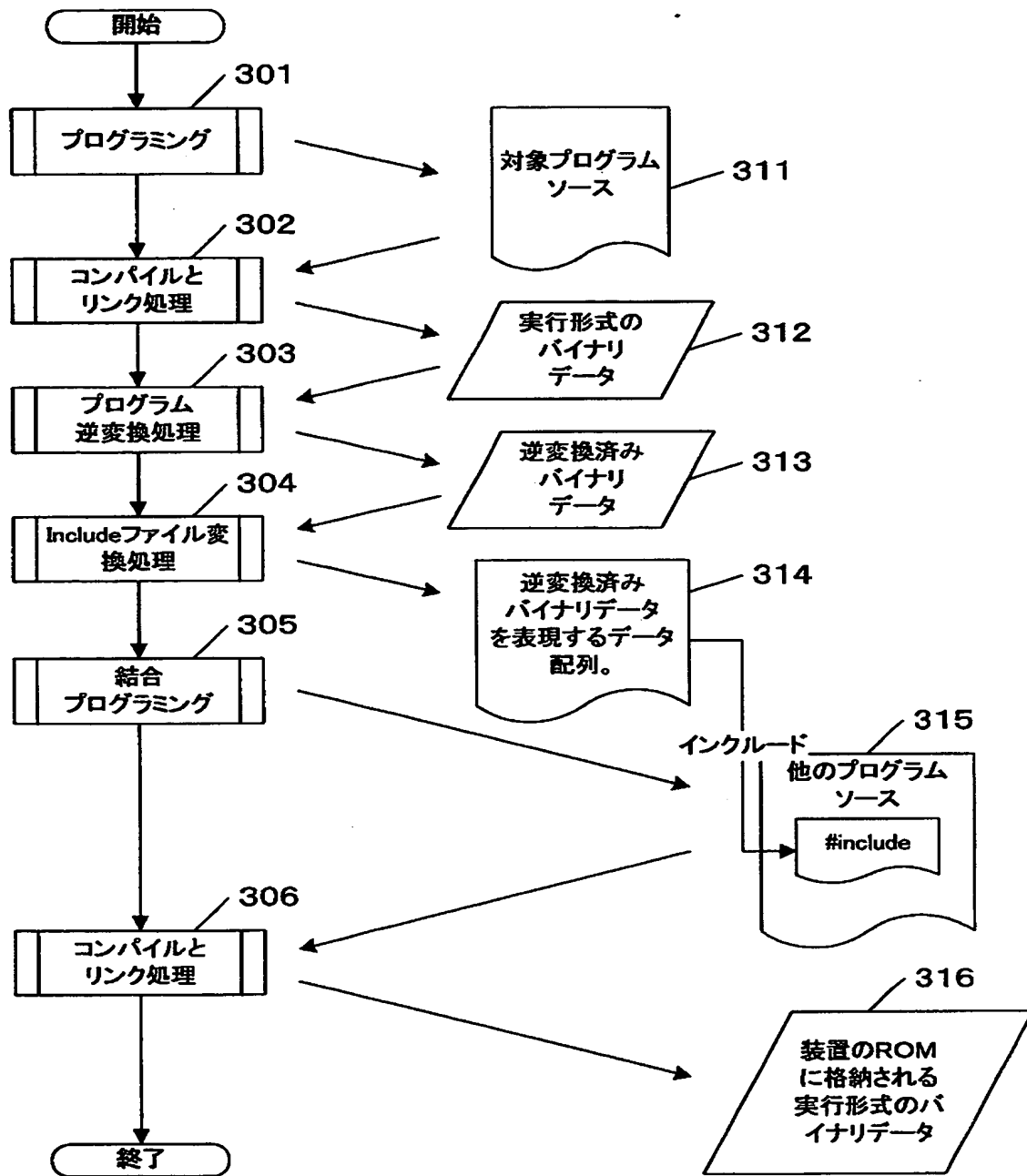
【図1】



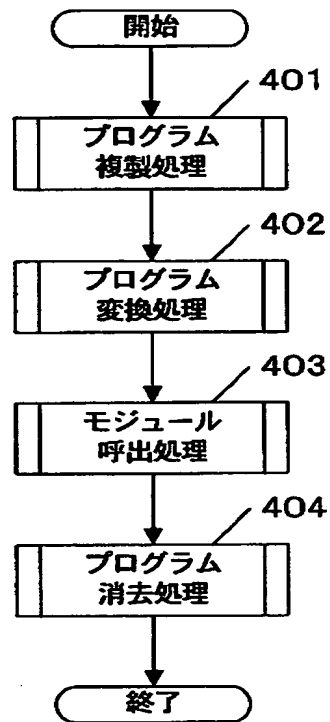
【図 2】



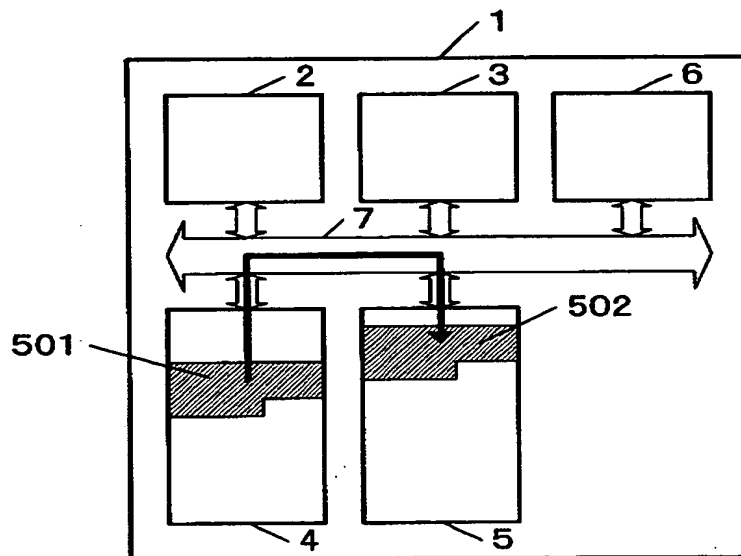
【図 3】



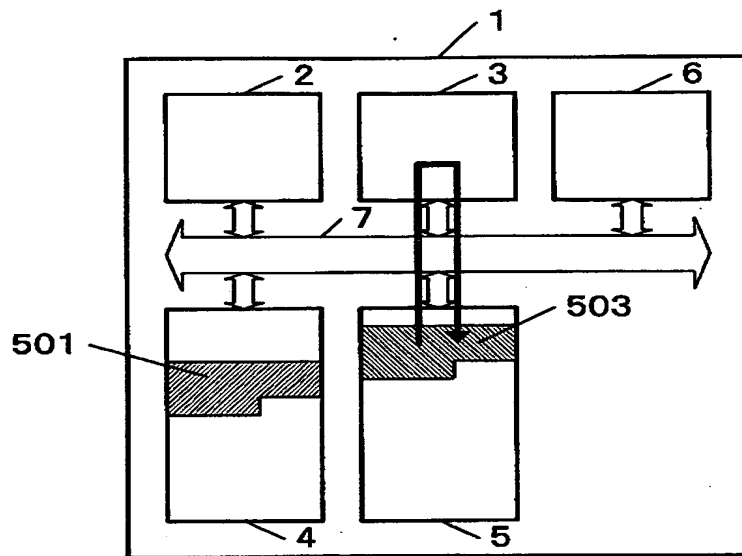
【図 4】



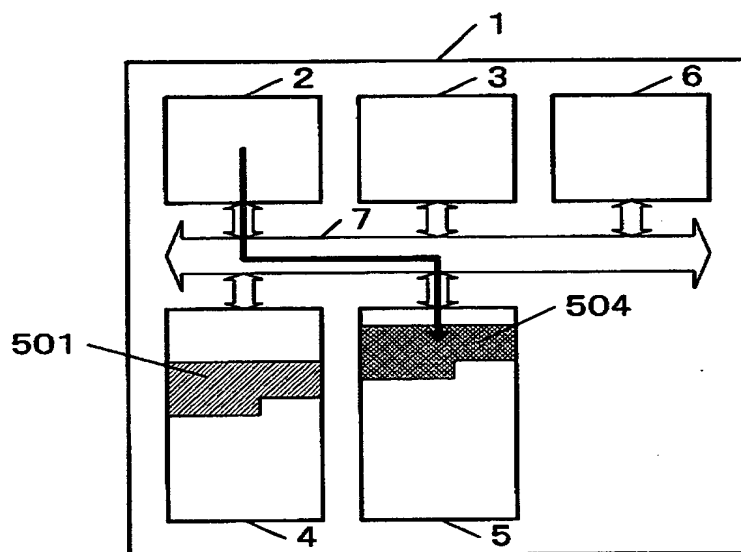
【図 5 A】



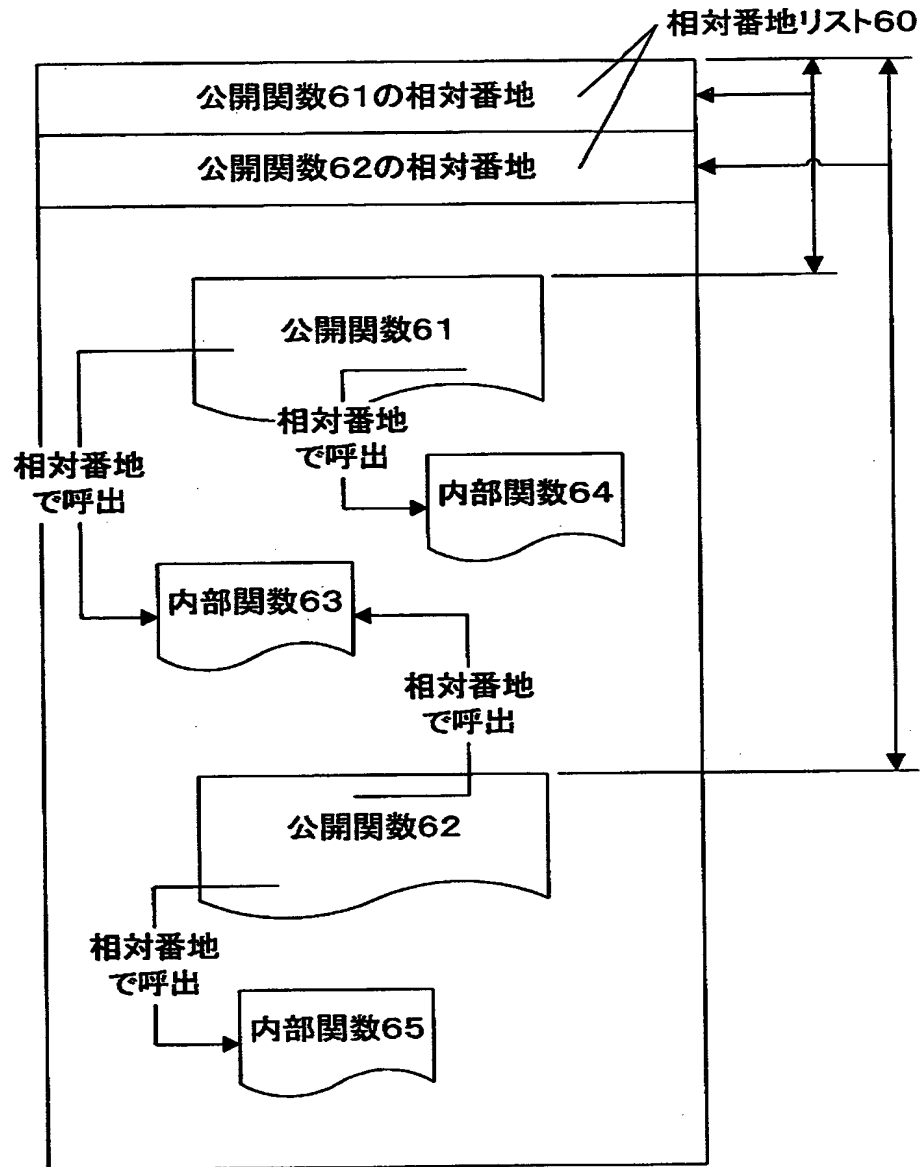
【図5B】



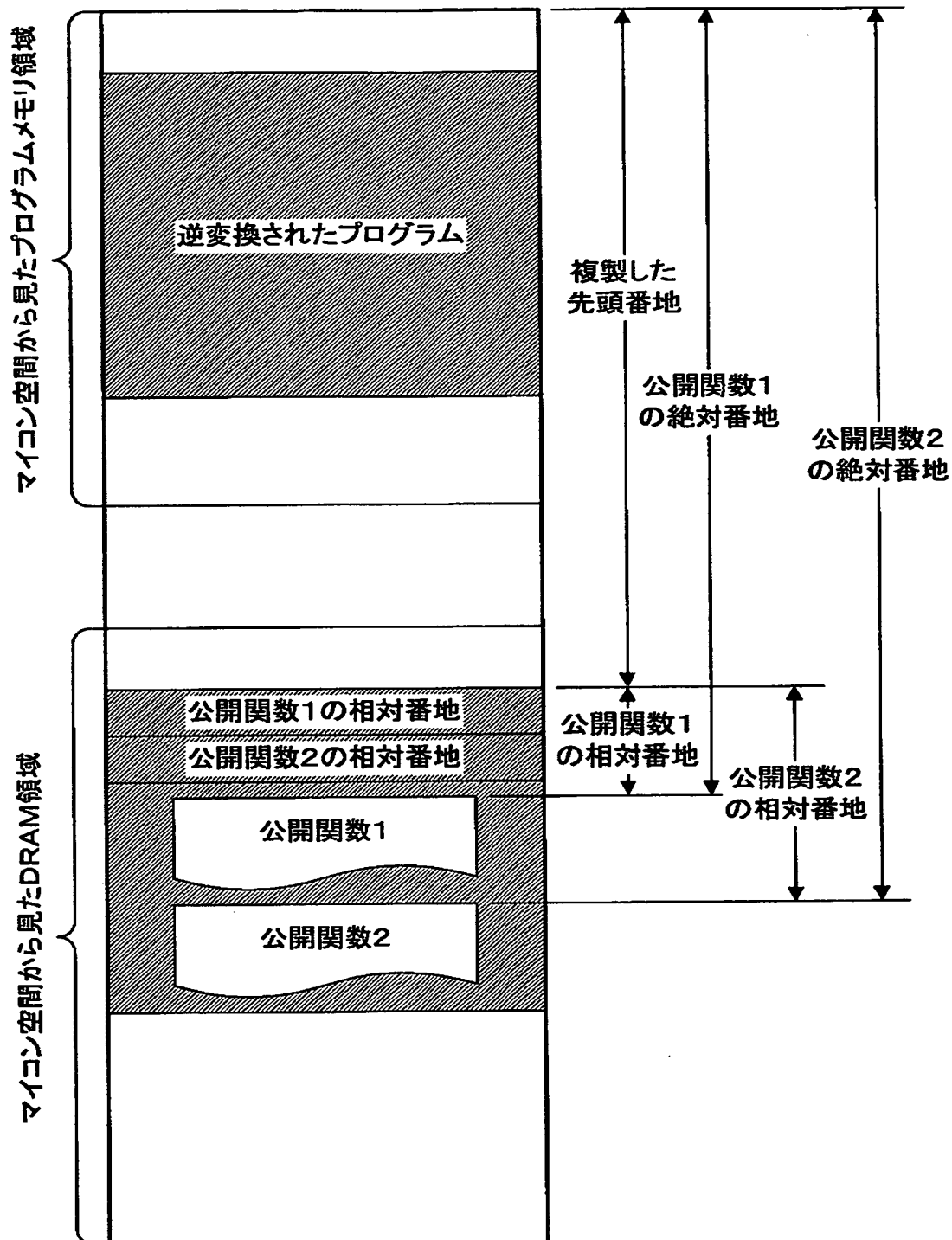
【図5C】



【図 6】



【図 7】



【書類名】 要約書

【要約】

【課題】 著作権保護機能などを装置に導入する場合、その機能自身を第三者による解読から守るために隠蔽する必要がある。L S I に機能を隠蔽する場合は、開発期間とコストがかかる。ソフトウェアに機能を隠蔽する場合は、隠蔽強度を持たせるのが困難である。

【解決手段】 装置に備わる可逆変換を行うデータ変換回路に着目し、隠蔽対象となる機能を実現する制御プログラムにデータ変換回路の逆変換を施してプログラムメモリに保存し、隠蔽対象の制御プログラムの復元処理をデータ変換回路で行う。従って、制御プログラムに自分自身の復元アルゴリズムが存在しないので、隠蔽強度を高めることができる。

【選択図】 図 3

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 8 2 1]

1. 変更年月日 1 9 9 0 年 8 月 2 8 日

[変更理由] 新規登録

住 所 大阪府門真市大字門真 1 0 0 6 番地

氏 名 松下電器産業株式会社